Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

1. Thông tin lỗ hổng bảo mật

- Mô tả: Lỗ hổng này tồn tại trong Spring Core, cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng: ứng dụng sử dụng Spring Core phiên bản JDK >= 9.0.

2. Hướng dẫn kiểm tra và khắc phục lỗ hổng

2.1. Hướng dẫn kiểm tra, xác định bị ảnh hưởng bởi lỗ hổng Srping4Shell

Bước 1: Kiểm tra phiên bản JDK

Trên máy chủ, hãy chạy lệnh "***java -version***" để kiểm tra phiên bản JDK đang chạy. Nếu phiên bản <= 8.0, hệ thống Quý đơn vị không bị ảnh hưởng bởi lỗ hổng này.

Bước 2: Kiểm tra việc sử dụng Spring Framework

1. Đối với hệ thống được triển khai dưới dạng war package:

- Giải nén war package

- Tìm kiếm tệp jar ở định dạng ***spring-beans-*.jar*** (ví dụ: spring-beans-5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Spring framework.

2. Đối với hệ thống được triển khai dưới dang jar package:

- Giải nén jar package

- Tìm kiếm tệp jar ở định dạng ***spring-beans-*.jar*** (ví dụ: spring-beans-5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Spring framework.

- Nếu không tìm thấy tệp ***spring-beans-*.jar***, hãy tiếp tục tìm kiếm tệp ***CachedIntrospectionResults.class*** trong tệp giải nén. Nếu tồn tại tệp này chứng tỏ hệ thống đang sử dụng Spring framework.

Bước 3: Phân tích, điều tra xác nhận

Sau khi hoàn thành 2 bước kiểm tra ở trên, các điều kiện sau được đáp ứng đồng thời sẽ xác định hệ thống bị ảnh hưởng bởi lỗ hổng bảo mật này:

- Phiên bản JDK >= 9.0

- Sử dụng Spring framework hoặc derived framework.

- Tồn tại endpoint sử dụng chức năng DataBinder.

2.2. Hướng dẫn khắc phục

Hiện tại, chưa có bản vá để khắc phục lỗ hổng bảo mật nói trên. Vì vậy, để giảm thiểu nguy cơ bị tấn công, Quý đơn vị có thể thực hiện các biện pháp khắc phục theo nguồn hướng dẫn tham khảo của một số tổ chức tại:

https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html

3. Nguồn tham khảo

https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html

https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-code.html